第 39 卷第 10 期
录用定稿
计算机应用研究
Application Research of Computers
Vol. 39 No. 10
Accepted Paper

安全增强的智能电网轻量级匿名认证方案

丁志帆[a]，胡洪波[a,b]，杨庆余[a]，肖思远[a]

(湘潭大学 a. 自动化与电子信息学院; b. 网络与信息管理中心, 湖南 湘潭 411105)

摘　要：现有的智能电网身份认证方案大多存在计算成本高和认证流程复杂的问题，不适用于智能电网中资源受限的智能设备。而一些轻量级的方案却存在各种安全漏洞，这些方案都无法在效率和安全性之间实现所需的权衡。针对上述问题，基于椭圆曲线加密算法设计了一个增强的可证明安全的智能电网轻量级匿名认证方案。引入辅助验证器，摆脱在认证阶段对于电力供应商的依赖，在保护智能电表真实身份的条件下实现网关和智能电表之间的相互认证。同时，可以通过伪身份对恶意智能电表进行身份的溯源和撤销。通过在随机预言模型下的安全性分析和仿真工具 ProVerif 证明了方案具备较高的安全属性。性能分析表明，所提方案能够满足智能电网环境下对于安全性和高效性的要求。

关键词：智能电网；身份认证；椭圆曲线；随机预言模型；ProVerif

中图分类号：TP309.2　　doi: 10.19734/j.issn.1001-3695.2022.03.0118

Security enhanced lightweight anonymous authentication scheme for smart grid

Ding Zhifan[a], Hu Hongbo[a, b], Yang Qingyu[a], Xiao Siyuan[a]

(*a. College of Electronic Information & Automation,b. Network & Information Management Center*, *Xiangtan University*, *Xiangtan Hunan* 411105, *China*)

Abstract: Most of the existing smart grid authentication schemes suffer from high computational costs and complex authentication processes, which are not suitable for resource-constrained smart devices in the smart grid, while some lightweight schemes suffer from various security vulnerabilities, none of which can achieve the required trade-off between efficiency and security. To solve these problems, this paper designed an enhanced provably secure smart grid lightweight anonymous authentication scheme based on elliptic curve encryption algorithm. Introducing auxiliary validator to get rid of the reliance on the power supplier in the authentication phase and to achieve mutual authentication between the gateway and the smart meter under the condition of protecting the true identity of the smart meter. In addition, the scheme can trace and revoke the identity of malicious smart meters through pseudo identity. Through the security analysis under the random oracle model and simulation tool ProVerif verifies that the proposed scheme has high security properties. Performance analysis shows that the proposed scheme can meet the requirements for security and efficiency in smart grid environment.

Key words: smart grid; identity authentication; elliptic curve; random oracle model; ProVerif

0　引言

传统的电力系统因其自身的局限性，已不足以应对新兴工业生产以及社会经济发展的挑战。智能电网作为下一代电力系统，将传感、计算和通信等先进技术嵌入电网中，以提供可行、高效、可持续、具有经济效益和安全的电力供应，显著提高现有电网的效率[1]。在发电端通过将可再生能源并入电网，智能电网可以实现更准确的监控、潮流优化和更环保的绿色能源发电[2]。在用户端为了实现对用户用电量的实时监控，智能电表等智能计量基础设施被部署在智能电网中，每个用户都配备一个智能电表，用于定期收集用户的用电数据，网关定期聚合区域内一组用户的用电数据，电力供应商分析聚合的用电数据并动态更新价格以实施用户侧管理[3]。

尽管智能电网有许多优点，但它的互连性和动态性以及对信息通信技术和网络系统的高度依赖使得智能计量基础设施容易受到许多安全威胁，如中间人攻击、假冒攻击和重放攻击等各类已知攻击[4]。由于电力供应商，网关和智能电表之间的通信是双向流动的，攻击者能够从多个入口渗入智能电网系统并窃取用户的用电数据信息，并进一步入侵电力供应商的电力数据库。因此，网络安全成为智能电网最关键的问题[5]。然而，传统的网络安全技术如密码保护、反恶意软件和防火墙等都有其自身的局限性[6]。为了解决这些问题，需要将安全高效的认证机制集成到智能电网的通信系统中，以支持通信实体之间安全的信息交换，同时保护其隐私。身份认证和密钥协商方案是安全高效的认证机制，能够保障智能电网各通信方的远程安全通信，实现数据机密性、用户隐私和消息完整性，为智能电网提供可靠的电力服务。

为了应对智能电网中存在的安全问题，研究人员近年提出了许多适用于智能电网的身份认证和密钥协商方案，但仍存在着两个主要问题：

a) 现有的方案大部分都被指出存在各种安全漏洞，容易遭受各类已知攻击，不能提供会话密钥的安全性或智能电表的匿名性，无法满足在智能电网环境下的安全需求。

b) 现有的一些方案由于使用了指数运算或双线性配对此类高开销的操作而导致了较高的计算和通信成本，而智能电表的资源十分有限，难以满足方案的需求。

最近，Gope 等人[7]提出一个空间数据聚合方案，用于在智能电网中安全获取电力需求，该方案包括两个阶段：认证

收稿日期：2022-03-28；**修回日期：**2022-05-14

作者简介：丁志帆(1998-)，男，广东潮州人，硕士研究生，主要研究方向为智能电网信息安全、密码学(202021002542@smail.xtu.edu.cn)；胡洪波(1972-)，男，湖南湘潭人，高级实验师，硕士，主要研究方向为电力物联网、智能电网信息安全；杨庆余(1997-)，男，湖南长沙人，硕士研究生，主要研究方向为智能电网隐私保护、雾计算；肖思远(1997-)，男，湖南娄底人，硕士研究生，主要研究方向为智能电网信息安全.

和数据聚合。他们声称其方案是安全的，在认证阶段能够实现安全的认证和密钥协商，并且具备对已知攻击的抵抗力，是智能电网环境的最佳选择。但是，本文发现该方案无法抵抗密钥泄露伪装攻击，并且其会话密钥是不安全的，这会严重影响智能电网通信系统的安全性。

为了解决上述问题，本文基于椭圆曲线加密算法，提出一种新的且可证明安全的智能电网轻量级匿名认证方案，能够满足智能电网环境的安全需求，在性能上也更具优势。本文的主要贡献有：

a) 对 Gope 等人方案中的认证阶段进行安全性分析，证明该方案无法抵抗密钥泄露伪装攻击,并且其会话密钥安全性薄弱。

b) 设计了适用于智能电网的身份认证和密钥协商方案，引入一个辅助验证器，使得电力供应商不介入方案的认证阶段。

c) 本文方案在消息认证时不暴露智能电表的身份信息，保证了智能电表的匿名性和不可追踪性，通过对称加密算法实现了轻量级的伪身份更新，特定情况下通过伪身份对恶意智能电表进行溯源和撤销。

d) 使用随机预言模型以及仿真工具 ProVerif 证明了会话密钥的安全性以及抵御各类已知攻击的能力，与相关方案对比分析显示所提方案在安全性，计算成本以及通信量三个方面都有优势。

1　相关研究

近年来已经提出了多种加密协议，包括数字签名、加密、数据聚合、安全数据存储和身份认证方案作为作为学术界和工业界保护智能电网安全的解决方案[8]，其中身份认证方案是保障智能电网数据安全和实施隐私保护的第一道防线，是智能电网部署的重要要求。2015 年，Tsai 和 Lo[9]采用双线性配对提出了基于身份的签名方案和基于身份的加密方案，实现了服务提供商和智能电表的相互认证。2016 年，Odelu 等人[10]中指出 Tsai 和 Lo 的方案[9]无法保证智能电表秘密凭证的隐私和会话密钥的安全性，并提出了一个安全高效的认证密钥协商方案，成功解决了 Tsai 和 Lo 的方案中存在的潜在隐私泄露问题。2017 年，Chen 等人[11]表明 Odeul 等人的方案[10]容易遭受假冒攻击，并且可以通过密钥生成中心追踪智能电表。为了解决文献[10]中的问题，Chen 等人改变了智能电表在密钥生成中心的注册方式，智能电表的身份在发送前被加密，并且智能电表的私钥不会泄露给密钥生成中心，因此不受密钥生成中心发起的各种潜在攻击的影响。然而，上述方案[9~11]使用了双线性配对和指数运算，并且存在密钥托管问题，因此会产生较高的计算成本。

为了满足轻量级的需求，越来越多的研究人员采用椭圆曲线加密算法(ECC)构建智能电网认证方案。2016 年，He 等人[12]为了降低 Tsai 和 Lo 的方案[9]中使用双线性配对和指数运算而导致的高计算成本，提出了一个基于椭圆曲线加密算法的轻量级匿名密钥协商方案，在没有可信第三方的情况下实现智能电表和服务供应商的相互认证。2018 年，Abbasinezhad 等人[13]指出 He 等人的方案[12]无法抵抗已知会话的临时信息攻击和智能电表的临时秘密值泄露攻击，并提出了一个基于椭圆曲线加密算法的密钥协商方案，能够提供会话密钥的安全性并且解决了以往方案的密钥托管问题，然而被指出缺乏智能电表的匿名性[14]。2020 年，Garg 等人[15]提出了一种安全的身份认证方案，将完全散列 Menezes-QuVanstone(FHMQV)密钥交换机制和椭圆曲线加密算法相结合，能够抵御各类已知攻击，计算成本低，但是被证明无法实现智能电表的匿名性和不可追踪性[16]。2021 年，Srinivas 等人[17]结合椭圆曲线加密算法和 Schnorr 的签名方案设计了一种新的基于匿名签名的认证密钥交换方案，支持在初始部署后添加新的动态智能电表，但是被指出无法抵抗中间人攻击和假冒攻击，并且不提供匿名功能[18]。

为了保护智能电表的匿名性，伪身份生成技术也在不断发展。2021 年，Azeem 等人[19]提出了一种用于智能电网需求响应管理的轻量级认证密钥方案，使用哈希散列函数生成伪身份以确保智能电网设备的匿名性，并且支持伪身份的更新。然而，由于哈希散列函数的单向不可逆，他们的方案不支持伪身份的溯源。2022 年，Safkhani 等人[20]提出一种智能电网的认证和密钥协商方案，使用物理不可克隆函数(PUF)和对称加密算法构建用户的伪身份保证了匿名性。但是，他们的方案不支持伪身份的更新和溯源。Gope 等人的方案[7]在智能电表上传用户用电数据前，电力供应商，智能电表和第三方聚合器进行身份认证，确保通信实体的合法性。该方案使用对称加密算法构建伪身份以提供智能电表的匿名性，具备对常见已知攻击的抵抗力，并且使用低成本的加密原语实现了通信实体之间的轻量级认证。然而，本文通过安全性分析发现，Gope 等人的方案无法抵抗密钥泄露伪装攻击，并且会话密钥安全性薄弱。

2　预备知识

本节主要介绍本文方案的困难性问题、系统模型等理解本文所需的知识。

2.1　困难性问题

椭圆曲线离散对数难题(ECDLP)：假设 q 是一个大素数，G 是一个阶为 q 的加法循环群，对于给定的 $P \in G$ 和 $a \cdot P \in G$，计算 $a \in Z_q^*$ 是困难的。

椭圆曲线 Diffile-Hellman 难题(ECDHP)：对于给定的 $P, a \cdot P, b \cdot P \in G$，其中 $a, b \in Z_q^*$，计算 $a, b \in Z_q^*$ 是困难的。

2.2　系统模型

如图 1 所示，在已有模型[7,21]的基础上提出本方案的系统模型，该模型中有 4 个通信实体：电力供应商(PS)，网关(GW)，相应家庭局域网中的智能电表(SM)，辅助验证器(AV)。

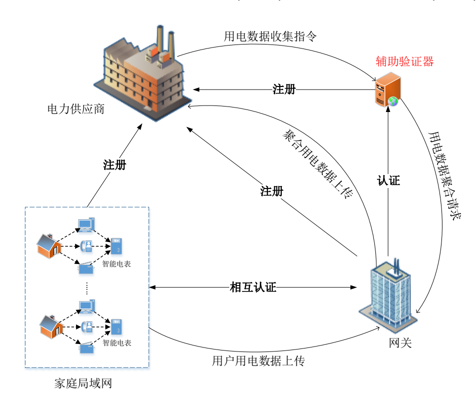


图 1　系统模型

Fig. 1　System model

a) 电力供应商(PS)。它是整个智能电网的管理员，主要负责生成和发放安全参数，对来自网关的聚合用电数据进行监控和分析并调整电价，与文献[7,21]相比，本方案中电力供应商只提供注册服务，不介入智能电表和网关的身份认证和密钥协商。

b) 网关(GW)。它具有庞大的存储空间和优秀的计算能力，收集并聚合来自其负责区域内家庭局域网的智能电表加密用电数据，将处理好的数据发送给电力供应商。这是一个诚实但对智能电表的加密用电数据好奇的半可信第三方实体，收到辅助验证器的用电数据聚合请求后，对其进行身份认证，认证通过即发起与智能电表的相互认证并建立会话密钥。

c) 智能电表(SM)。它是智能电网的终端设备，负责定期收集并加密用户的用电数据，这是一种资源受限的智能设备，存储空间和计算能力有限。

d) 辅助验证器(AV)。它是一个第三方智能防窜改设备，向电力供应商注册获取相关安全参数，收到电力供应商的用电数据收集指令后，向网关发送用电数据聚合请求，网关需对其认证后方才同智能电表协商会话密钥。

2.3 安全目标

一个安全高效的智能电网身份认证和密钥协商方案需为通信实体提供良好的安全性，应实现以下安全目标：

a) 相互认证：为确保智能电表的数据上传给授权合法的网关以及网关接收来自合法智能电表的加密用电数据，在智能电表和网关之间应能提供相互认证。

b) 智能电表的匿名性不可追踪性：确保攻击者无法追踪到智能电表的真实身份以及智能电表在通信网络中的任何活动踪迹。

c) 会话密钥的前向安全性：即使攻击者获得网关和智能电表的长期秘密参数，也能确保先前已建立会话密钥的安全性。

d) 抵抗密钥泄露伪装攻击：即使网关或智能电表一方的私钥泄露，攻击者也无法伪装成私钥泄露方同另一方进行密钥协商。

e) 抵抗各类已知的攻击：能够抵抗假冒攻击，重放攻击，中间人攻击和智能电表临时秘密值泄露攻击。

2.4 攻击者模型

本文结合 Dolev-Yao 威胁模型和 CK 攻击者模型，构造了一个强大的攻击者，其在概率多项式时间内具有以下能力：

a) A 可以任意窃听，拦截，修改，删除，注入通信通道上的消息。

b) A 可以获取系统先前的会话密钥。

c) 在评估对密钥泄露伪装攻击的抵抗时，A 可以获取通信实体的私钥。

3 Gope 等人方案的安全性分析

在本节中，回顾了 Gope 等人方案的认证阶段，并分析该方案存在的安全漏洞。

3.1 Gope 等人方案认证阶段的回顾

电力供应商(PS)为家庭局域网内的每个智能电表(SM_i)生成伪身份 PID_i 和私钥 k_i，并与第三方聚合器(TPA)共享私钥 K_{as}。在收集用户用电数据聚合前，电力供应商,第三方聚合器,智能电表进行三方之间的相互认证，下面是具体过程。

a) SM_i 生成随机数 N_s，计算 $V_0=h\{PID_i \| N_s \| k_i\}$，将消息 $M_{A_1}:\{PID_i,N_s,V_0\}$ 发送给 TPA。

b) TPA 生成随机数 N_a,计算 $V_1=h\{ID_A \| N_a \| K_{as}\}$，发送消息 $M_{A_2}=\{(PID_i,N_s,V_0)\|(ID_A,N_a,V_1)\}$ 给 PS。

c) PS 依据伪身份 PID_i 在数据库中找寻对应 SM_i 的真实身份 ID_{SM_i}，并验证 V_0 和 V_1 的正确性，验证通过则表明 PS 认证了 SM_i 和 TPA 的身份，为 SM_i 生成新的伪身份 PID_i^{new}，计算 $T=h(ID_{SM_i}\|K_{as}\|N_s)$，$x=h(k_i\|T\|N_s)\oplus h(K_{as}\|N_a)$，$y=h(T\|N_s\|k_i)\oplus N_a$，$z=h(T\|ID_{SM_i}\|k_i)\oplus PID_i^{new}$，$V_2=h(K_{as}\|N_a\|x)$，$V_3=h(T\|y\|z\|k_i)$，发送消息 $M_{A_3}:\{x,y,z,V_2,V_3\}$ 给 TPA。

d) TPA 验证 V_2 的正确性，验证通过后计算 $TK=x\oplus h(K_{as}\|N_a)$，生成会话密钥 $kh_i=h(TK\|N_a\|N_s)$，生成一组 SM_i 的临时身份 $TID_{iq}=\{tid_{i1}, tid_{i2},\cdots,tid_{iq}\}$，使用 kh_i 加密 TID_{iq} 即 $TID_{iq}^*=E_{kh_i}[TID_{iq}]$，计算 $V_4=h(TID_{iq}^*\|kh_i\|ID_A)$，存储 $\{TID_{iq},kh_i\}$，并发送消息 $M_{A_4}:\{(y,z,V_3)\|(TID_{iq}^*,V_4)\}$ 给 SM_i。

e) SM_i 计算 $T=h(ID_{SM_i}\|K_{as}\|N_s)$，验证 V_3 的正确性，验证通过即认证了 PS 的身份，计算 $N_a=h(T\|N_a)\oplus k_i\oplus y$，$TK=h(k_i\|T\|N_s)$，$kh_i=h(TK\|N_s\|N_a)$，$PID_i^{new}=h(T\|ID_{SM_i}\|k_i)\oplus z$，验证 V_4 的正确性，验证通过即认证了 TPA 的身份，最后 SM_i 使用 kh_i 解密 TID_{iq}^* 获得 TID_{iq}，存储参数 $\{PID_i^{new},TID_{iq},kh_i\}$。

3.2 Gope 等人方案的安全漏洞

本节展示 Gope 等人方案的认证阶段无法抵抗 **2.4** 节构建的攻击者 A 进行的密钥泄露伪装攻击，且无法提供会话密钥的安全性。

攻击者 A 窃听 TPA 和 SM_i 以及 TPA 和 PS 之间的通信通道，并获取参数 $\{PID_i,N_s,V_0\}$ 和 $\{ID_A\}$，根据密钥泄露伪装攻击的假设[22],攻击者可以获取 PS 和 TPA 的共享私钥 K_{as}，伪装成 TPA，同 PS 进行会话。具体攻击过程如下。

a) A 窃听并拦截消息 $M_{A_1}:\{PID_i,N_s,V_0\}$ 和 $\{ID_A\}$，生成随机数 N_A，计算 $V_A=h(ID_A\|N_A\|K_{as})$,发送消息 $M_{A_2}=\{(PID_i,N_s,V_0)\|(ID_A,N_A,V_A)\}$ 给 PS。

b) PS 依据伪身份 PID_i 在数据库中找寻对应 SM_i 的真实身份，并验证 V_0 和 V_A 的正确性，验证通过则表明 PS 认证了 SM_i 和 A 的聚合器身份，为 SM_i 生成新的伪身份 PID_i^{new}，计算 $T=h(ID_{SM_i}\|K_{as}\|N_s)$，$x=h(k_i\|T\|N_s)\oplus h(K_{as}\|N_A)$，$y=h(T\|N_s\|k_i)\oplus N_A$，$z=h(T\|ID_{SM_i}\|k_i)\oplus PID_i^{new}$，$V_2=h(K_{as}\|N_A\|x)$，$V_3=h(T\|y\|z\|k_i)$，发送消息 $M_{A_3}:\{x,y,z,V_2,V_3\}$ 给 A。

c) A 验证 V_2 的正确性，验证通过后计算 $TK=x\oplus h(K_{as}\|N_A)$，生成会话密钥 $kh_i=h(TK\|N_A\|N_s)$，伪造一组 SM_i 的临时身份 $TID_{iAq}=\{tid_{iA1},tid_{iA1},\cdots,tid_{iAq}\}$，使用 kh_i 加密 TID_{iAq} 即 $TID_{iAq}^*=E_{kh_i}[TID_{iAq}]$，计算 $V_4=h(TID_{iAq}^*\|kh_i\|ID_A)$ 并存储 $\{TID_{iAq},kh_i\}$，发送消息 $M_{A_4}:\{(y,z,V_3)\|(TID_{iAq}^*,V_4)\}$ 给 SM_i。

d) SM_i 计算 $T=h(ID_{SM_i}\|K_{as}\|N_s)$，验证 V_3 的正确性，验证通过即认证了 PS 的身份，计算 $N_A=h(T\|N_A)\oplus k_i\oplus y$，$TK=h(k_i\|T\|N_s)$，$kh_i=h(TK\|N_s\|N_A)$，$PID_i^{new}=h(T\|ID_{SM_i}\|k_i)\oplus z$，验证 V_4 的正确性，验证通过即认证了 A 聚合器身份，最后 SM_i 使用 kh_i 解密 TID_{iAq}^* 获得 TID_{iAq}，存储参数 $\{PID_i^{new},TID_{iAq},kh_i\}$。

综上，A 成功伪装成 TPA 同 PS 和 SM_i 进行会话，可见 Gope 等人的方案无法抵抗密钥泄露伪装攻击，并且在 PS 和 TPA 的共享私钥 K_{as} 丢失的情况下，A 能够成功计算出会话密钥 kh_i，所以 Gope 等人的方案无法提供会话密钥的安全性。

4 提出的方案及正确性证明

为了抵抗文献[7]存在的安全漏洞，并确保智能电网的通信安全，本文提出了一个增强的且可证明安全的身份认证和密钥协商方案。该方案由初始化、注册、身份认证和密钥协商以及恶意智能电表撤销四个阶段组成。

4.1 初始化

在此阶段，电力供应商 PS 初始化生成以下参数：

a) 选择大素数 p，q，基于 F_p 选择一条椭圆曲线 E，F_p 表示为模 p 的有限域，选择点 P 为椭圆曲线 E 上阶为 q 的基点。

b) 选择随机数 $sk_{PS}\in Z_q^*$ 作为 PS 的私钥，计算 $pk_{PS}=sk_{PS}\cdot P$ 作为 PS 的公钥。

c) 选取安全的单向哈希散列函数 h。

d) 定义一种对称加密算法 $Enc_{(k)}$，使得 $Dec_{(k)}(Enc_{(k)}(message))=message$，其中 k 是加密和解密的密钥，$Dec_{(k)}$ 是对称解密，$message$ 为需要被加密的参数。

最后公布参数 $\{p,q,E,P,pk_{PS},h,Enc_{(k)}\}$。

4.2 注册

在此阶段，辅助验证器(AV)，网关(GW)和第 i 个智能电表(SM_i)通过电力供应商(PS)进行注册，生成下一阶段所需的参数，通过秘密通道进行传输。

4.2.1 AV 注册

AV 选定身份标识符 ID_{AV} 发送给 PS 请求注册，PS 选择随机数 $sk_{GW}\in Z_q^*$ 返回，AV 选择随机数 $r_{AV}\in Z_q^*$，计算 $R_{AV}=h(sk_{GW}\|r_{AV})$ 并将 $\{r_{AV},R_{AV}\}$ 发送给 PS 完成注册。

4.2.2 GW 注册

a) GW 在 AV 注册完成后即选定身份标识符 ID_{GW} 发送给 PS 请求注册。

b) PS 计算 $R_{GW}=h(sk_{GW}\|ID_{GW})\cdot P$，选择随机数 $r_{PS}\in Z_q^*$，生成 GW 的签名 $s_{GW}=h(R_{GW}\|ID_{GW})sk_{PS}+r_{PS}$，计算 $B_1=h(ID_{AV}\|pk_{PS})$，$B_2=r_{AV}\oplus B_1$，$B_3=h(ID_{GW}\|ID_{AV})\oplus r_{PS}$，$V_{AV}=h(R_{AV}\|r_{PS})$ 作为 AV 的认证令牌，为第 i 个智能电表 SM_i 选定身份标识符 ID_{SMi}，将参数 $\{sk_{GW},s_{GW},B_2,B_3,V_{AV},ID_{SMi}\}$ 发送给 GW。

c) GW 将 sk_{GW} 作为私钥，计算 $pk_{GW}=sk_{GW}\cdot P$ 作为公钥，存储参数 $\{B_2,B_3,V_{AV},ID_{SMi},sk_{GW},s_{GW},pk_{GW}\}$，选择随机数 $r_{PID}\in Z_q^*$，利用私钥 sk_{GW} 加密 SM_i 的真实身份标识符 ID_{SMi}，生成 SM_i 的伪身份 $PID_{SMi}=Enc_{sk_{GW}}(ID_{SMi}\|r_{PID})$ 并将其发送给 PS 完成注册。

4.2.3 SM_i 注册

PS 在 GW 注册完成后生成 SM_i 的签名 $s_{SMi}=h(PID_{SMi}\|s_{GW})sk_{PS}$，将参数 $\{s_{SMi},ID_{SMi},PID_{SMi},ID_{GW}\}$ 发送给 SM_i，SM_i 选择随机数 $r_{SMi}\in Z_q^*$，计算 $sk_{SMi}=r_{SMi}s_{SMi}$，$pk_{SMi}=r_{SMi}\cdot pk_{PS}$ 分别作为私钥和公钥，最后存储参数 $\{ID_{SMi},ID_{GW},sk_{SMi},pk_{SMi},PID_{SMi}\}$ 注册完成。

4.3 身份认证和密钥协商

在此阶段，辅助验证器 AV 向网关 GW 发送用户用电数据聚合请求，网关 GW 对辅助验证器 AV 进行身份认证，验证通过即发起与智能电表 SM_i 的相互认证并协商会话密钥。

a) AV 将 ID_{SMi} 发送给 GW，GW 计算 $B_1=h(ID_{AV}\|pk_{PS})$，$r_{AV}=B_1\oplus B_2$，$R_{AV}=h(sk_{GW}\|r_{AV})$，$r_{PS}=h(ID_{GW}\|ID_{AV})\oplus B_3$，验证 $h(R_{AV}\|r_{PS})=V_{AV}$ 是否成立，成立则 AV 身份验证通过。GW 选择随机数 $q_{GW}\in Z_q^*$，计算 $Q_{GW}=q_{GW}\cdot pk_{GW}$，将消息 $M_1:\{Q_{GW}\}$ 发送给 SM_i。

b) SM_i 选择一个随机数 $q_{SMi}\in Z_q^*$，计算 $Q_{SMi}=q_{SMi}\cdot pk_{SMi}$，$k_{SG}=sk_{SMi}q_{SMi}\cdot Q_{GW}$，生成认证令牌 $V_{SMi}=h(k_{SG})\oplus h(ID_{SMi}\|ID_{GW})$，将消息 $M_2:\{PID_{SMi},Q_{SMi},V_{SMi}\}$ 发送给 GW。

c) GW 计算 $k_{GS}=Q_{SMi}\cdot q_{GW}sk_{GW}h(PID_{SMi}\|s_{GW})$，验证 $h(k_{GS})\oplus h(ID_{SMi}\|ID_{GW})=V_{SMi}$ 是否成立，成立则 SM_i 身份验证通过。GW 选择随机数 $r_{PID}^{new}\in Z_q^*$，利用私钥 sk_{GW} 对 SM_i 的伪身份进行解密，即 $(ID_{SMi}\|r_{PID})=Dec_{sk_{GW}}(PID_{SMi})$，得到 SM_i 的真实身份标识符 ID_{SMi}，并为 SM_i 生成一个新的伪身份 $PID_{SMi}^{new}=Enc_{sk_{GW}}(ID_{SMi}\|r_{PID}^{new})$，生成会话密钥 $SK_{GS}=h(Q_{SMi}\|Q_{GW}\|k_{GS})$，计算 $XP=PID_{SMi}^{new}\oplus h(SK_{GS})$，生成认证令牌 $V_{GW}=h(PID_{SMi}^{new}\|SK_{GS})\oplus h(ID_{SMi}\|ID_{GW})$，将消息 $M_3:\{XP,V_{GW}\}$ 发送给 SM_i。

d) SM_i 生成会话密钥 $SK_{SG}=h(Q_{SMi}\|Q_{GW}\|k_{SG})$，计算 $PID_{SMi}^{new}=XP\oplus h(SK_{SG})$，验证等式 $h(PID_{SMi}^{new}\|SK_{SG})\oplus h(ID_{SMi}\|ID_{GW})=V_{GW}$ 是否成立，成立则 GW 身份验证通过，SM_i 更新自己的伪身份 PID_{SMi}^{new} 用于下一次认证。

最后 GW 和 SM_i 存储会话密钥 SK（$SK_{GS}=SK_{SG}$）用于它们之间的进一步交互。

4.4 恶意智能电表撤销

当 GW 检测到其管辖区域内的智能电表存在恶意行为，如发送错误的认证信息或电力消费数据异常等，向 PS 提出身份溯源请求。PS 对该智能电表的数据和行为进行审核后，将恶意智能电表的伪身份 PID_{SMi} 发送给 GW 进行溯源。由于智能电表的伪身份是由 GW 生成的，所以只有 GW 能够对智能电表的伪身份进行溯源。

GW 利用私钥 sk_{GW} 对恶意智能电表的伪身份 PID_{SMi} 进行解密锁定其真实身份，并将其通过秘密通道传输给 PS，PS 将恶意智能电表的真实身份和伪身份一起添加到撤销列表中，通信系统中的所有成员均可查询撤销列表以避免与列表中的恶意智能电表交互。

4.5 正确性证明

证明 GW 生成的会话密钥 $SK_{GS}=h(Q_{SMi}\|Q_{GW}\|k_{GS})$ 与 SM_i 生成的会话密钥 $SK_{SG}=h(Q_{SMi}\|Q_{GW}\|k_{SG})$ 相等，需要证明 k_{GS} 与 k_{SG} 相等，证明过程由以下方程式示出。

$$\begin{aligned}k_{GS}&=Q_{SMi}\cdot q_{GW}sk_{GW}h(PID_{SMi}\|s_{GW})=\\&pk_{SMi}\cdot q_{SMi}q_{GW}sk_{GW}h(PID_{SMi}\|s_{GW})=\\&pk_{PS}\cdot r_{SMi}q_{SMi}q_{GW}sk_{GW}h(PID_{SMi}\|s_{GW})=\\&P\cdot sk_{PS}r_{SMi}q_{SMi}q_{GW}sk_{GW}h(PID_{SMi}\|s_{GW})=\\&r_{SMi}h(PID_{SMi}\|s_{GW})sk_{PS}q_{SMi}q_{GW}sk_{GW}\cdot P\end{aligned}$$

$$\begin{aligned}k_{SG}&=sk_{SMi}q_{SMi}\cdot Q_{GW}=\\&r_{SMi}s_{SMi}q_{SMi}\cdot Q_{GW}=\\&r_{SMi}h(PID_{SMi}\|s_{GW})sk_{PS}q_{SMi}\cdot Q_{GW}=\\&r_{SMi}h(PID_{SMi}\|s_{GW})sk_{PS}q_{SMi}q_{GW}\cdot pk_{GW}=\\&r_{SMi}h(PID_{SMi}\|s_{GW})sk_{PS}q_{SMi}q_{GW}sk_{GW}\cdot P\end{aligned}$$

5 随机预言模型下形式化安全性分析

使用安全模型进行形式化分析成为现代密码学中强有力的安全证明之一。在现有的安全模型中，本文使用随机预言模型来执行本方案的形式化分析。

5.1 随机预言安全模型

本方案的身份认证和密钥协商阶段，SM_i 和 GW 是两个主要的参与者，假设每个 SM_i 和 GW 能够运行多个会话，S_i 表示 SM_i 的第 i 个会话实例，G_j 表示 GW 的第 j 个会话实例，每个会话实例都被称为一个预言机。当攻击者对预言机发起预言查询时，预言机需要返回相应的响应参数。定义实例 $o\in\{S_i,G_j\}$，在随机预言模型中，o 代表两个会话实例 S_i 和 G_j 之一。概率多项式时间内的攻击者 A 可以任意窃听，拦截，修改，删除，注入通信通道上的消息，其攻击能力由以下预言查询体现。

$Extract(o)$：此查询用于模拟 A 的被动攻击，A 可以获取各个通信方在公共通信通道上的所有消息。

$send(o,M)$：此查询用于模拟 A 的主动攻击，A 将在通信通道上获取到的消息 M 发送给 o，o 将相应的消息返回。

$Corrupt(o)$：此查询使 A 获取实例 o 的长期秘密参数。

$Test(o)$：此查询用于模拟实例 o 会话密钥的语义安全性。进行 $Test(o)$ 查询后，o 抛掷一个硬币 b，如果 b=1(硬币为正面)，o 将会话密钥返回给 A，如果 b=0 (硬币为反面)，则返回给 A 一个随机字符串，其长度跟会话密钥相等。

安全性定义：本方案的安全性通过游戏 $G_i(i=0,1,2,3,4,5)$ 进行评估。在游戏中 A 可以对 o 发起多次 $Test(o)$ 查询，收到查询后 o 抛掷硬币 b (结果为 0 或 1)，如果 A 正确猜中 b 值，则认为 A 赢得游戏，将攻击者 A 攻破本方案 S 安全性的优势定义为

$$Adv_S(A)=|2Pr[Succ_A]-1|<\varepsilon \tag{1}$$

其中，$Pr[Succ_A]$ 是 A 在游戏 G_i 中猜中 b 值的概率，ε 是一个及其小可忽略的值。

5.2 安全分析

定理 1　攻击者 A 在概率多项式时间内赢得游戏 G_i 的概率是可以忽略的，A 最多能够执行 q_h 次哈希查询，q_s 次 $Send$ 查询以及 q_e 次 $Execute$ 查询，A 攻破方案 S 安全性的最大优势为

$$Adv_S(A)=\frac{q_h^2}{|Hash|}+\frac{(q_s+q_e)^2}{p}+2(\frac{q_s}{|Hash|}+Adv_{E(k)}(A)+Adv_{ECDLP}(A)) \tag{2}$$

其中，$|Hash|$ 是哈希查询的规模，$Adv_{E(k)}(A)$ 表示 A 违反对称加密算法 $Enc_{(k)}$ 的优势，$Adv_{ECDLP}(A)$ 表示概率多项式时间内 A 解决 ECDLP 的优势。

证明　通过游戏 $G_i(i=0,1,2,3,4,5)$ 推导 A 攻破本方案 S 的优势，$Pr[Succ_i]$ 表示 A 猜中游戏 G_i 中硬币 b 值的概率。

游戏 G_0：该游戏模拟的是真实的攻击场景，得到

$$Adv_S(A)=|2Pr[Succ_0]-1| \tag{3}$$

游戏 G_1：该游戏通过执行 $Extract(o)$ 查询模拟 A 的被动攻击。A 通过窃听得到消息 $M_1:\{Q_{GW}\}$，$M_2:\{PID_{SMi},Q_{SMi},V_{SMi}\}$，$M_3:\{XP,V_{GW}\}$，但是 A 无法通过这些消息计算会话密钥 SK。所

以在该游戏结束时，A 进行 $Test(o)$ 查询无法判断 o 返回的参数是真实的会话密钥还是等长随机字符串。因此，与真实的攻击场景相比，A 在该游戏中并没有增加优势，所以有

$$Pr[Succ_0]=Pr[Succ_1] \quad (4)$$

游戏 G_2：该游戏去除游戏 G_1 中存在的两种碰撞情形，模拟 A 的主动攻击。

情形 1　根据生日悖论[23]，哈希查询的输出发生碰撞，其概率小于等于 $q_h^2/2|Hash|$。

情形 2　选取的随机数发生碰撞，其概率小于等于 $(q_s+q_e)^2/2p$。

除非发生上述碰撞，否则 G_2 与 G_1 不可区分，因此有

$$Pr[Succ_2]-Pr[Succ_1]\le \frac{q_h^2}{2|Hash|}+\frac{(q_s+q_e)^2}{2p} \quad (5)$$

游戏 G_3:该游戏去除游戏 G_2 中 A 无须进行哈希查询而猜测到认证令牌 V_{SMi} 或 V_{GW} 的情形，这种情形的概率小于等于 $q_s/|Hash|$。因此有

$$Pr[Succ_3]-Pr[Succ_2]\le \frac{q_s}{|Hash|} \quad (6)$$

游戏 G_4:该游戏去除游戏 G_3 中 A 对 PID_{SMi} 成功解密获得 ID_{SMi} 的情形，因此有

$$Pr[Succ_4]-Pr[Succ_3]\le Adv_{E(k)}(A) \quad (7)$$

游戏 G_5：该游戏对游戏 G_4 进行修改，模拟 A 的密钥泄露伪装攻击。在该游戏中 A 执行 $Extract(o)$ 查询获取通信通道上的参数，执行 $Corrupt(o)$ 查询获得 S_i 和 G_j 的长期秘密参数。在已知 $\{sk_{SMi},Q_{GW},Q_{SMi},pk_{SMi}\}$ 的情况下，要想获得 S_i 的会话密钥 $SK_{SG}=h(Q_{SMi}\|Q_{GW}\|k_{SG})$，需要计算 $k_{SG}=sk_{SMi}q_{SMi}\cdot Q_{GW}$，但从 $Q_{SMi}=q_{SMi}\cdot pk_{SMi}$ 中得到 q_{SMi} 需要解决椭圆曲线离散对数难题(ECDLP)，对于 G_j 同理。因此，比较该游戏与游戏 G_4 的区别可以得出

$$Pr[Succ_5]-Pr[Succ_4]\le Adv_{ECDLP}(A) \quad (8)$$

在该游戏中，A 在猜测 b 值上并没有增加优势，因此

$$Pr[Succ_5]=\frac{1}{2} \quad (9)$$

根据式(3)和(4)，得到

$$\frac{1}{2}Adv_S(A)=|Pr[Succ_0]-\frac{1}{2}|=|Pr[Succ_1]-\frac{1}{2}| \quad (10)$$

根据式(9)和(10)，得到

$$\frac{1}{2}Adv_S(A)=|Pr[Succ_1]-Pr[Succ_5]| \quad (11)$$

根据式(5)~(8)和三角不等式，得到

$$\begin{aligned}&|Pr[Succ_1]-Pr[Succ_5]|=\\&|Pr[Succ_1]-Pr[Succ_2]+Pr[Succ_2]-Pr[Succ_3]+\\&Pr[Succ_3]-Pr[Succ_4]+Pr[Succ_4]-Pr[Succ_5]|\le\\&|Pr[Succ_1]-Pr[Succ_2]|+|Pr[Succ_2]-Pr[Succ_3]|+\\&|Pr[Succ_3]-Pr[Succ_4]|+|Pr[Succ_4]-Pr[Succ_5]|\le\\&\frac{q_h^2}{2|Hash|}+\frac{(q_s+q_e)^2}{2p}+\frac{q_s}{|Hash|}+Adv_{E(k)}(A)+Adv_{ECDLP}(A)\end{aligned} \quad (12)$$

根据式(11)和(12),得到式(2)

$$Adv_S(A)=\frac{q_h^2}{|Hash|}+\frac{(q_s+q_e)^2}{p}+2(\frac{q_s}{|Hash|}+Adv_{E(k)}(A)+Adv_{ECDLP}(A))$$

由此，定理一证毕。以上证明过程意味着 A 在游戏中获胜的概率是可忽略的，因此，本方案在随机预言模型下是安全的。

6　ProVerif 仿真分析

ProVerif 是一个被广泛使用的自动化密码协议仿真工具，支持多种密码学原语，如加密、解密、数字签名、散列函数等，并指定了重写规则和方程式。该工具能够证明可达性、认证性以及观测等效性。它由三个部分组成，即协议输入、系统处理和结果输出，系统输入部分是运用 Pi 演算或 Horn 逻辑来编码的协议，系统处理部分是运用一阶逻辑对编码的协议的安全性进行推导，结果输出部分能够在编码的协议不满足某种特定的安全属性时给出相应的攻击序列。此外，ProVerif 中还具有一个攻击者模型，可以进行窃听、拦截、修改或重新传输消息，这些攻击仅受到加密方法的限制。

本文将所提方案在 ProVerif 中建模为四个不同的场景，以便证明所提方案对已知攻击的抵抗能力，并且进一步验证方案具备智能电表的匿名性和会话密钥的前向安全性。

在场景一中，没有泄露任何的秘密参数，仅对方案在 ProVerif 中进行建模，对一些常见的攻击进行查询，证明了智能电表的匿名性和方案的可达性，仿真结果如图 2 所示，结果①是对方案可达性的查询，证明了会话密钥的安全性；结果②证明了智能电表的匿名性；结果③和④表明智能电表和网关可以进行相互认证，并且能够抵抗假冒、重放、中间人等常见的攻击。

```
Completing equations...
Completing equations...
-- Process 1-- Query not attacker(SK) in process 1
Completing...
200 rules inserted. Base: 175 rules (40 with conclusion selected). Queue: 44 rules.
400 rules inserted. Base: 364 rules (62 with conclusion selected). Queue: 37 rules.
Starting query not attacker(SK)
RESULT not attacker(SK) is true.                                              ①
-- Query not attacker(IDSMi[]) in process 1
Completing...
200 rules inserted. Base: 175 rules (40 with conclusion selected). Queue: 44 rules.
400 rules inserted. Base: 364 rules (62 with conclusion selected). Queue: 37 rules.
Starting query not attacker(IDSMi[])
RESULT not attacker(IDSMi[]) is true.                                         ②
-- Query inj-event(endSMi) ==> inj-event(startSMi) in process 1
Completing...
200 rules inserted. Base: 171 rules (33 with conclusion selected). Queue: 42 rules.
400 rules inserted. Base: 358 rules (58 with conclusion selected). Queue: 88 rules.
Starting query inj-event(endSMi) ==> inj-event(startSMi)
RESULT inj-event(endSMi) ==> inj-event(startSMi) is true.                     ③
-- Query inj-event(endGW) ==> inj-event(startGW) in process 1
Completing...
200 rules inserted. Base: 176 rules (33 with conclusion selected). Queue: 37 rules.
400 rules inserted. Base: 365 rules (62 with conclusion selected). Queue: 57 rules.
Starting query inj-event(endGW) ==> inj-event(startGW)
RESULT inj-event(endGW) ==> inj-event(startGW) is true.                       ④
```

图 2　场景一的仿真验证结果

Fig. 2　Simulation results of scenario 1

在场景二中，验证本方案具备会话密钥的前向安全性，使用命令 $((!pGW)|(!pPS)|(!pSMi)|(!pAV)|(phase1;out(net,(pkSMi,pkGW,skSMi,skGW,sGW))))$ 向攻击者泄露会话密钥中的长期秘密参数，查询结果如图 3 所示，攻击者获取会话密钥失败。

```
Completing equations...
Completing equations...
-- Process 1-- Query not attacker_p1(SK) in process 1
Completing...
200 rules inserted. Base: 180 rules (59 with conclusion selected). Queue: 31 rules.
400 rules inserted. Base: 364 rules (89 with conclusion selected). Queue: 70 rules.
Starting query not attacker_p1(SK)
RESULT not attacker_p1(SK) is true.
```

图 3　场景二的仿真验证结果

Fig. 3　Simulation results of scenario 2

在场景三中，验证本方案具备密钥泄露伪装攻击的抵抗力，使用命令 $((!pGW)|(!pPS)|(!pSMi)|(!pAV)|(phase2;out(net,(skSMi,skGW))))$ 向攻击者泄露智能电表和网关的私钥，查询结果如图 4 所示，攻击者获取会话密钥失败。

```
Completing equations...
Completing equations...
-- Process 1-- Query not attacker_p2(SK) in process 1
Completing...
200 rules inserted. Base: 179 rules (73 with conclusion selected). Queue: 41 rules.
400 rules inserted. Base: 363 rules (105 with conclusion selected). Queue: 69 rules.
600 rules inserted. Base: 556 rules (115 with conclusion selected). Queue: 19 rules.
Starting query not attacker_p2(SK)
RESULT not attacker_p2(SK) is true.
```

图 4　场景三的仿真验证结果

Fig. 4　Simulation results of scenario 3

在场景四中，验证本方案具备智能电表临时秘密值泄露的抵抗力，使用命令 $((!pGW)|(!pPS)|(!pSMi)|(!pAV)|(phase3;out(net,(qSMi,QSMi))))$ 向攻击者泄露智能电表的临时秘密值，查询结果如图 5 所示，攻击者获取会话密钥失败。

7　性能分析

本节从安全性，计算成本以及通信量三个方面对本方案

进行性能分析，将本方案与文献[7,9,10,12,17,19,20]的方案进行比较。

```
Completing equations...
Completing equations...
-- Process 1-- Query not attacker_p3(SK_GW_SMI[]) in process 1
Completing...
200 rules inserted. Base: 184 rules (75 with conclusion selected). Queue: 36 rules.
400 rules inserted. Base: 374 rules (107 with conclusion selected). Queue: 71 rules.
600 rules inserted. Base: 566 rules (112 with conclusion selected). Queue: 14 rules.
Starting query not attacker_p3(SK_GW_SMI[])
RESULT not attacker_p3(SK_GW_SMI[]) is true.
```

图 5　场景四的仿真验证结果

Fig. 5　Simulation results of scenario 4

如表 1 所示，在安全性上，本方案能够提供相互认证、智能电表的匿名性和不可追踪性、会话密钥的安全性以及抵抗各类已知的攻击。Gope 等人方案[7]无法提供相互认证和会话密钥的安全性，并且无法抵抗密钥泄露伪装攻击。其他文献[9,10,12,17,19,20]的方案也均存在各种安全缺陷，因此就安全性而言，本方案优于现有方案。

采用文献[24]在 Ubuntu12.04.1 LTS 32 位操作系统上获得的实验结果对比 8 个方案在认证阶段的计算成本。哈希操作的计算成本 $T_h \approx 0.0023$ms；对称加/解密的计算成本 $T_{ed} \approx 0.0046$ms；ECC 点乘的计算成本 $T_m \approx 2.226$ms；ECC 点加的计算成本 $T_a \approx 0.0288$ms；指数运算的计算成本 $T_e \approx 3.85$ms；双线性配对的计算成本为 $T_p \approx 5.811$ms，个别操作由于计算成本过低忽略不计[25]。通信量是协议执行期间通过网络传输的总位数，较低的通信量可提供更快的数据传输和更少的时间延迟，为了计算通信量，假设身份标识，随机数，哈希散列输出，时间戳，对称加/解密块等为 160 bit；椭圆曲线上的点为 320 bit；双线性映射组的生成元 G_1 为 1024 bit。表 2 为计算成本和通信量的对比结果。

在计算成本方面，本方案主要采用哈希散列函数和二进制运算此类轻量级运算，同时辅以 ECC 点乘运算和对称加/解密运算，计算成本为 8.9523ms。文献[9,10]采用双线性配对运算和指数运算，大幅增加了计算量。文献[12,17,20]主要采用 ECC 点乘运算，然而 ECC 点乘运算的使用次数均超过本方案。本方案的计算成本相比于文献[9,10,12,17,20]分别减少了 74.4%，70.8%，60.0%，33.4%，42.7%。Gope 等人方案[7]主要采用哈希散列函数构建其认证方案，没有额外的高成本运算，计算成本较低。然而由表 1 可知，Gope 等人方案[7]由于使用轻量级的加密原语导致其安全性不足，容易遭受安全攻击。

表 1　安全性对比

Tab. 1　Safety comparison

方案	P1	P2	P3	P4	P5	P6	P7	P8
文献[9]	√	√	√	√	√	√	×	×
文献[10]	√	√	√	√	×	√	√	×
文献[12]	√	√	√	√	√	√	×	×
文献[17]	√	×	×	√	×	√	√	×
文献[19]	√	√	√	√	√	√	×	×
文献[20]	√	√	√	√	√	√	√	×
文献[7]	×	√	√	√	√	×	√	×
本文方案	√	√	√	√	√	√	√	√

注：P1 相互认证 P2 智能电表匿名性和不可追踪性 P3 抗中间人攻击 P4 抗重放攻击 P5 抗假冒攻击 P6 会话密钥的前向安全性 P7 抗智能电表临时秘密值泄露攻击 P8 抗密钥泄露伪装攻击。

在通信量方面，本方案在保证安全性的情况下将认证阶段的消息传输次数减少至 3 次，实现了通信过程的精简化，通信量仅为 1760 bit。而 Gope 等人方案[7]在认证阶段的消息传输次数为 4 次，通信量达到了 3040 bit。本方案的通信量相比于文献[7,9,10,12,17,19]分别减少了 42.1%，50.5%，52.6%，21.4%，15.4%，9.0%，大大降低了通信时延。

由表 1 和 2 可知，本方案在提供足够安全性的同时，也能够保证较低的计算成本和通信量。Gope 等人方案[7]足够轻量级，然而却存在安全性不足和认证流程复杂进而导致通信量过高的问题，无法兼顾高效性和安全性。此外，Gope 等人的方案不支持伪身份的更新和溯源，而本方案 *GW* 在会话中能够生成新的智能电表伪身份 PID_{SMi}^{new} 并发放给 SM_i，SM_i 则更新伪身份用于下一次会话。同时，本方案能够通过伪身份溯源恶意智能电表的真实身份并将其撤销。

表 2　计算成本和通信量对比

Tab. 2　Calculation time and traffic comparison

方案	操作	计算成本/ms	通信量/bit
文献[9]	$10T_h+7T_m+2T_a+2T_e+2T_p$	34.9846	3552
文献[10]	$12T_h+5T_m+6T_a+2T_e+2T_p$	30.6524	3712
文献[12]	$11T_h+10T_m+3T_a$	22.3717	2240
文献[17]	$14T_h+6T_m+2T_a$	13.4458	2080
文献[19]	$18T_h$	0.0414	1920
文献[20]	$7T_h+7T_m+8T_{ed}$	15.6349	1440
文献[7]	$22T_h+2T_{ed}$	0.0598	3040
本文方案	$12T_h+7T_{ed}+4T_m$	8.9523	1760

8　结束语

本文针对现有智能电网通信认证方案安全性不足和效率低的问题，分析证明了 Gope 等人方案的安全漏洞，并基于椭圆曲线加密算法提出了一个适用于智能电网的身份认证和密钥协商方案，通过仿真工具 ProVerif 和理论分析验证了所提方案的安全性，与同类认证方案对比表明，所提方案在安全性，计算成本和通信量三个方面均具有优势，能够满足智能电网在通信过程中对于安全性和高效性的要求。

本方案仅支持网关对智能电表进行一对一的单点认证，网关的计算成本与其管辖区域内的智能电表数量成线性关系。在智能电表部署愈发完善的情况下，网关可能在同一时间段需要进行大量的认证服务，这将会导致很高的网络时延，并且对网关的计算能力也是一个极大的考验。下一步将研究单个网关对多个智能电表进行批量认证以减少网关的计算负担。

参考文献：

[1] Sadhukhan D, Ray S, Obaidat M S, *et al.* A secure and privacy preserving lightweight authentication scheme for smart-grid communication using elliptic curve cryptography [J]. Journal of Systems Architecture, 2021, 114: 101938.

[2] Ferrag M A, Maglaras L A, Janicke H, *et al.* A systematic review of data protection and privacy preservation schemes for smart grid communications [J]. Sustainable Cities and Society, 2018, 38: 806–835.

[3] Mahmood K, Chaudhry S A, Naqvi H, *et al.* A lightweight message authentication scheme for smart grid communications in power sector [J]. Computers & Electrical Engineering, 2016, 52 (C): 114-124.

[4] Li Xiong, Wu Fan, Saru K, *et al.* A provably secure and anonymous message authentication scheme for smart grids [J]. Journal of Parallel and Distributed Computing, 2019, 132: 242-249.

[5] Dua A, Kumar N, Singh M, *et al.* Secure message communication among vehicles using elliptic curve cryptography in smart cities [C]// Proc of the International Conference on Computer Information and Telecommunication Systems. Kunmin, NJ: IEEE Press, 2016: 1–6.

[6] Wang Wenye, Lu Zhou. Cyber security in the smart grid: survey and challenges [J]. Computer Networks, 2013, 57 (5): 1344–1371.

[7] Gope P, Sikdar B. Lightweight and privacy-friendly spatial data aggregation for secure power supply and demand management in smart grids [J]. IEEE Trans on Information Forensics and Security, 2019, 14

(6): 1554-1566.

[8] Wu Libing, Wang Jing, Sherali Z, *et al.* Anonymous and efficient message authentication scheme for smart grid [J]. Security and Communication Networks, 2019: 1-12.

[9] Tsai J L, Lo N W. Secure anonymous key distribution scheme for smart grid [J]. IEEE Trans on Smart Grid, 2016, 7 (2): 906-914.

[10] Odelu V, Das A K, Wazid M, *et al.* Provably secure authenticated key agreement scheme for smart grid [J]. IEEE Trans on Smart Grid, 2018, 9 (3): 1900-1910.

[11] Chen Yuwen, Martínez J F, Castillejo P, *et al.* An anonymous authentication and key establish scheme for smart grid: FAuth [J]. Energies, 2017, 10 (9): 1354-1377.

[12] He Debiao, Wang Huaqun, Khan M K, *et al.* Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography [J]. Iet Communications, 2016, 10 (14): 1795-1802.

[13] Abbasinezhad M D, Ostad S A, Nikooghadam M. *et al.* A secure and efficient key establishment scheme for communications of smart meters and service providers in smart grid [J]. IEEE Trans on Industrial Informatics, 2020, 16 (3): 1495-1502.

[14] Fan Wu, Xu Lili, Li Xiong, *et al.* A lightweight and provably secure key agreement system for a smart grid with elliptic curve cryptography [J]. IEEE Systems Journal, 2019, 13 (3): 2830-2838.

[15] Garg S, Kaur K, Kaddoum G, *et al.* Secure and lightweight authentication scheme for smart metering infrastructure in smart grid [J]. IEEE Trans on Industrial Informatics, 2020, 16 (5): 3548-3557.

[16] Fatty S, Osama E. A lightweight authenticated key establishment scheme for secure smart grid communications [J]. International Journal of Safety and Security Engineering, 2020, 10 (4): 549-558.

[17] Srinivas J, Das A K, Li Xiong, *et al.* Designing anonymous signature-based authenticated key exchange scheme for internet of things-enabled smart grid systems [J]. IEEE Trans on Industrial Informatics, 2021, 17 (7): 4425-4436.

[18] Tanveer M, Khan A U, Shah H, *et al.* ARAP-SG: Anonymous and reliable authentication protocol for smart grids [J]. IEEE Access, 2021, 9: 143366-143377.

[19] Azeem I, Shehzad A C, Mamoun A, *et al.* A secure demand response management authentication scheme for smart grid [J]. Sustainable Energy Technologies and Assessments, 2021, 48: 101571.

[20] Safkhani M, Kumari S, Shojafar M, *et al.* An authentication and key agreement scheme for smart grid [J]. Peer-to-Peer Networking and Applications, 2022, 15: 1595–1616.

[21] Huang Chengpeng, Wang Xiaoming, Gan Qingqing, *et al.* A lightweight and fault-tolerable data aggregation scheme for privacy-friendly smart grids environment [J]. Cluster Computing, 2021, 24: 3495–3514.

[22] Daniel R M, Rajsingh E B, Silas S. An efficient eCK secure identity based two party authenticated key agreement scheme with security against active adversaries [J]. Information and Computation, 2020, 275: 104630.

[23] 齐小晨，黎妹红，杜晔. 多服务器环境下基于动态 ID 的轻量级身份认证协议 [J]. 北京航空航天大学学报, 2021, 47 (12): 2632-2640. (Qi Xiaochen, Li Meihong, Du Ye. Lightweight identity authentication protocol based on dynamic ID in multi-server environment [J]. Journal of Beijing University of Aeronautics and Astronautics, 2021, 47 (12): 2632-2640.)

[24] Kilinc H H, Yanik T. A survey of sip authentication and key agreement schemes [J]. IEEE Communications Surveys & Tutorials, 2014, 16 (2): 1005-1023.

[25] 李晓天，陈建华. 更安全的匿名三因子多服务器身份认证协议研究 [J]. 计算机应用研究, 2020, 37 (9): 2781-2788. (Li Xiaotian, Chen Jianhua. Research on security-enhanced three-factor multi-server authentication scheme with anonymity [J]. Application Research Of Computers, 2020, 37 (9): 2781-2788.)